REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-9, 11-20, 22, 23, and 25-35 are pending in the present patent application. Claims 1, 17, 18, 34, and 35 are independent. The remaining claims depend, either directly or indirectly, from claims 1 and 18.

Claim Amendments

Claims 1, 17, 18, 34, and 35 have been amended for clarification. No new matter has been added by way of these amendments as support for these amendments may be found, for example, in Figure 4, Figure 7, and paragraphs [0031], [0037], and [0038] of the published specification.

Drawings

Applicant respectfully requests the Examiner acknowledge the formal drawings filed on March 22, 2002 and indicate whether they are acceptable.

Information Disclosure Statement (IDS)

Applicant respectfully requests the Examiner acknowledge and consider the references in the IDS filed contemporaneously with this response.

Examiner Interview

Applicant respectfully requests an Examiner Interview on August 1, 2006 at 2:00PM (EST). An Applicant Initiated Interview Request Form is enclosed with this submission.

Rejections under 35 U.S.C. § 101

Claims 18-20 and 22-34 stand rejected under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. By way of this reply, independent claims 18 and 34 have been amended to recite "wherein the encrypted serialized file provides secure storage of the key and the key encryption key on a server." Applicant respectfully asserts claims 18-20 and 22-34 involve the transformation of data (*i.e.*, serializing the vector to obtain an encrypted serialized file) using a computer into a tangible, useful, and concrete result (*i.e.*, secure storage of the key and key encryption key on a server). Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 1-9 and 11-17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,673,316 issued to Auerbach et al. (hereinafter "Auerbach"), in view of U.S. Patent No. 5,892,900 issued to Ginter et al. (hereinafter "Ginter I"), in further view of U.S. Patent No. 6,658,568 issued to Ginter et al. (hereinafter "Ginter II"). For the reasons set forth below, this rejection is respectfully traversed.

Amended independent claim 1 recites, in part, "a memory storing data in a n-tuple within the key management system, wherein the n-tuple comprises a distinct key name field, a distinct key value field, and a distinct key type field; an encryption module encrypting data, wherein the encryption module encrypts the distinct key name field, the distinct key value field,

and the distinct key type field using a key encryption key; a hashing module hashing the key encryption key." Amended independent claim 17 recites similar limitations. The Examiner has attempted to equate the n-tuple as recited in the claims, with the Bill of Material (BOM) as disclosed by Auerbach. (*See* Office Action dated March 29, 2006 at page 2). The Examiner has also attempted to equate the n-tuple as recited in the claims, with the document part and control part of a cryptographic envelope as disclosed by Auerbach. (*See* Office Action dated March 29, 2006 at page 8). Even assuming *arguendo* that either of these associations is proper, neither of these associations disclose each and every limitation of the amended claims.

Auerbach discloses a cryptographic envelope including a BOM. The BOM has a chart listing each part of the cryptographic envelope and the corresponding secure hash of each part. (*See* Auerbach at column 5, lines 13-34 and at Figure 3). The BOM also contains a digital signature, which is generated by encrypting the secure hash of each part with a document server (DS) secret key.

Applicant acknowledges that the chart of the BOM listing each part of the cryptographic envelope may include the name and type of an encryption key. Even assuming *arguendo* that the name and/or the type of the encryption key as disclosed by Auerbach are equivalent to the distinct key name field and the distinct key value field recited by the claims, Auerbach does not teach or suggest ***encrypting*** the name and the type of the encryption key ***using a key encryption key*** (KEK). Thus, the chart of the BOM cannot be read to be equivalent to the n-tuple, as recited in the claims, without the Examiner improperly reading the chart of the BOM unreasonably broad.

Auerbach also discloses a cryptographic envelope containing a document part and a control part. (*See* Auerbach at Figure 2). Applicant acknowledges that the document part and

the control part disclosed by Auerbach are encrypted using one or more encryption keys and that these encryption keys are encrypted (using the DS secret key) and stored as part of the cryptographic envelope. (*See* Auerbach at column 5, lines 8-12). However, neither the document part nor the control part (encrypted or non-encrypted) ever ***contain the name of an encryption key and/or the type of an encryption key***, squarely contradicting independent claims 1 and 17. Accordingly, the document part and the control part as taught by Auerbach cannot be read to be the n-tuple, as recited in the claims, without the Examiner mischaracterizing these terms.

Further, Applicant respectfully asserts Auerbach is silent regarding the key encryption key (KEK). As recited by the claims, the KEK is used to encrypt the n-tuple comprising the key name field, the key type field, and the key value field. The KEK is also hashed by the hashing module. Even if an attempt is made to associate the DS secret key as disclosed by Auerbach with the KEK, the DS secret key ***is never used to encrypt the name and the type of an encryption key***, and the DS secret key itself ***is never hashed***, contradicting what is explicitly recited in independent claims 1 and 17. Accordingly, Auerbach does not and cannot teach or suggest the KEK and the use of the KEK as recited in the claims.

Both Ginter I and Ginter II are silent regarding the n-tuple, the encryption of the n-tuple with the key encryption key (KEK), and the hashing of the KEK as recited in the claims. Thus, both Ginter I and Ginter II fail to teach or suggest what Auerbach lacks.

Auerbach, Ginter I, and Ginter II, whether viewed separately or in combination, fail to teach and suggest each and every limitation of amended independent claims 1 and 17. Thus, amended independent claims 1 and 17 are patentable over Auerbach, Ginter I, and Ginter II.

Claims 2-9 and 11-16 depend, either directly or indirectly, from claim 1 and are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 18-20 and 22-35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Auerbach in view of U.S. Patent No. 6,757,903 issued to Havemose (hereinafter "Havemose"). For the reasons set forth below, this rejection is respectfully traversed.

Amended independent claim 18 recites, in part, "combining data into a n-tuple comprising a distinct key name field, a distinct key value field, and a distinct key type field; encrypting the n-tuple comprising the distinct key name field, the distinct key value field, and the distinct key type field using the key encryption key to produce a secret token; ...hashing the key encryption key." Amended independent claims 34 and 35 recite similar limitations. As discussed above, Auerbach does not teach or suggest the n-tuple, the encryption of the n-tuple with the key encryption key (KEK), and the hashing of the KEK, as recited in the claims. Accordingly, Auerbach does not teach or suggest each and every limitation of amended independent claims 18, 34, and 35.

Havemose is silent regarding the n-tuple, the encryption of the n-tuple with the key encryption key (KEK), and the hashing of the KEK as recited in the claims. Thus, Havemose does not teach or suggest what Auerbach lacks.

Havemose and Auerbach, whether viewed separately or in combination, fail to teach or suggest every limitation of amended independent claims 18, 34, and 35. Thus, amended independent claims 18, 34, and 35 are patentable over Havemose and Auerbach. Claims 19, 20,

22, 23, and 25-33 depend, either directly or indirectly, from claim 18 and are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09469/010001).

Dated: June 29, 2006

Respectfully submitted,

ALY DOSSA L0031

By _____
for Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

Enclosures — Applicant Initiated Interview Request
IDS